Ministry of Defence

de&s

DE&S SAFETY AND ENVIRONMENTAL PROTECTION LEAFLET 14/2019

SYSTEM SAFETY RISK MANAGEMENT

Sponsor: DES TECH-QSEP-Hd	**Version: Issue 1.1**	**Date of Issue: Feb 2019**
Author: DES TECH-QSEP-Saf-AsstHd		
Contact: 030 679 35525		

1. The Acquisition Safety and Environmental Management System (ASEMS) requires DE&S projects, working in conjunction with the Duty Holder, to adopt a risk-based approach to safety management that systematically employs structured methods to identify hazards, assess the levels of associated risk then reduce residual risks to levels that are As Low As Reasonably Practicable (ALARP). The risk-based approach provides for flexibility in the tools, techniques and methodologies used at each stage, allowing adoption of those most suited to the specific system and application. Justification of the selected approach will then form an essential part of the safety argument presented in the Safety Case Report.

2. A review conducted after a recent fatal accident has identified potential shortcomings in how some DE&S project teams undertake safety management activities. These include:

a) **Use of inappropriate tools and processes;**
Suitable and sufficient risk assessments are vitally important to underpin safety case arguments. Appropriate risk management tools and techniques must be selected, and the choice documented and justified in Safety and Environmental Management Plans. Failure to apply suitably robust tools and techniques can have severe consequences, including the failure to identify or fully consider risks which need to be controlled. For complex systems, DE&S expects risk assessments to be conducted using structured techniques that are recognized as good practice, such as Failure Mode Effects (and Criticality) Analysis (FMEA/FMECA), Fault Tree Analysis (FTA), Hazard and Operability Studies (HAZOPS) and/or bow tie analysis. The ASEMS Toolkit gives overviews of these techniques.

b) **Lack of stakeholder involvement in key activities and decisions;**
To gain a full, clear and accurate understanding of how equipment is being used, project teams must involve equipment end users in key safety activities and decision making. We need honest feedback on the use of equipment and systems through-life, especially if this departs from defined procedures. DE&S is not responsible for providing this feedback,

but we are obliged to request it from operators and challenge them when it is inadequate.

c) **Excessive reliance on non-engineered mitigations such as Personal Protective Equipment (PPE) and procedures;**
Project teams must be extremely cautious of relying on procedural controls to mitigate safety risks. The risk of human failure, particularly in high-stress situations, can be significant. The selection of appropriate PPE must be fully assessed and documented and undertaken with the full involvement of user community representatives who can provide an accurate and up-to-date definition of the actual operating environment. Design of procedures needs similar involvement, to ensure users can effectively carry them out in all necessary scenarios (including maintenance and disposal, as well as training and normal in-service operation). Methods such as Bow Tie analysis can help avoid over-reliance on non-engineered controls, by graphically illustrating where risks are solely managed by administrative controls or PPE. Human Factors Integration (HFI) techniques can be used throughout the risk management process to help identify risks and balance the human and technological aspects of a capability. Further information is on the Knowledge in Defence HFI pages.

d) **Poor maintenance and review of the safety argument through-life.**
Safety arguments must be regularly reviewed and challenged throughout the life of the equipment. Risk assessments should be intensively scrutinised, considering not just the results but also fundamental aspects such as the validity of the tools and techniques employed to identify the hazards and assess the risks. It is good practice to undertake fresh analysis, targeted at specific parts of the safety argument, to determine whether the same conclusions are reached.

3. These shortcomings can have the most serious implications. Failure to identify and mitigate credible accident sequences, single point or common mode failures, or the potential for omission of critical components, can ultimately have catastrophic consequences. Assessments based on unrepresentative operating scenarios or conditions may compromise the effectiveness of control measures. For us to fully and competently discharge our safety responsibilities, it is essential our safety risk management activities are effective, fit for purpose and properly applied.

4. Annex A gives guidance on safety risk management throughout the project lifecycle. It builds on and complements the instructions published in the Project Oriented Safety Management System (POSMS) and the ASEMS Toolkit, both of which can be found at asems.mod.uk. It advises on the factors to consider when selecting the most appropriate risk management approach, emphasises the importance of considering risk reduction measures in a hierarchical manner, and reinforces the need to generate robust and auditable ALARP safety arguments.

Released under the authority of:

DE&S DSEQT QSEP-SEP DepHd

Annex:
A – Additional guidance on safety risk management

Additional Guidance on System Safety Risk Management

1. **Risk management** is not simply about reducing risk: it is defined in Def Stan 00-056 as "the systematic identification, evaluation and reduction of risk". Traditionally it breaks down into the three main elements shown in Figure 1:

- Risk Analysis;
- Risk Assessment; and
- Risk Control.

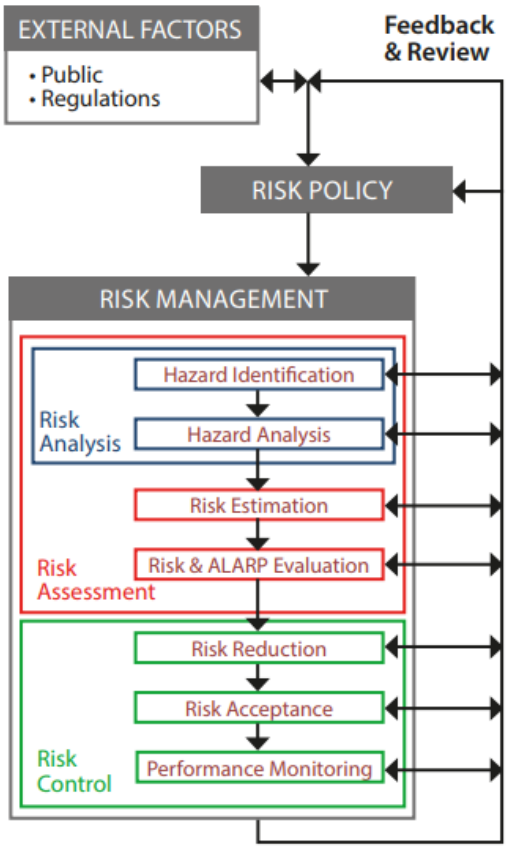

Figure 1. Elements of Risk Management

2. Risk management is an iterative process. It should be repeated through a system's lifecycle as knowledge about it develops. Although risk management relies on judgement, decisions should be based on the application of qualitative assessment methods, complemented where necessary by quantitative methods, particularly for systems which have the potential to present high levels of risk. Ultimately, the effort expended should be proportionate to the risks involved, with care needed when dealing with novel technologies and unusual applications. However, the legal requirement for risk assessments to be suitable and sufficient remains.

3. Risk management is part of safety management, but risk management activities have no effect on safety until the process of risk reduction is implemented.

For example, through risk analysis and assessment a project team may identify a cost-effective design change to reduce risk. However, this activity has no safety benefit until the design change is implemented.

4. The involvement of appropriate stakeholders, including end user representatives, is vital if the outcome of the risk management process is to be realistic, credible and comprehensive. For stakeholders to be effective, they must have sufficient knowledge relating to their relevant area of responsibility, be that design, maintenance, operation or support. That knowledge should be gained from actual, current experience which can inform the risk management process, and the stakeholder must have the moral courage to highlight areas where the real-life situation deviates from the approved or expected standard. Examples of this may be local work-arounds which bypass safety control measures, repeated failures of equipment or process which are not captured in reporting systems, or shortages of personnel with the necessary skills to ensure activities are conducted to the correct standard.

5. The three main elements of risk management, and their associated sub-elements, are described in more detail below.

Risk Analysis

6. Risk analysis involves applying structured methods to identify potential hazards (HAZID) and analysing how they might credibly be caused and lead to accidents (HAZAN). For most projects, the process starts with high-level Preliminary Hazard Identification and Analysis (PHIA). PHIA is undertaken at Concept stage or as early in the lifecycle as practical (see SMP04 in POSMS). The initial PHIA session will focus on the content of the Concept of Use (CONUSE) and the User Requirements Document (URD). At this stage, even before a design has been generated, we can identify the main hazards that might arise from the capability using informal techniques like brainstorming sessions or Structured What-If Technique (SWIFT) analysis. A potential level of severity can be established by asking questions like “Could a potential solution pose a credible risk to life?” and “Can the solution be solely responsible for that outcome?”.

7. Once the PHIA is complete, the project can move forward to a more detailed Hazard Identification and Analysis (HIA, see SMP05), assisted by more formal tools. These can also be used at the PHIA stage if appropriate. Hazard checklists, historic accident reports, operator experience and lessons identified from previous similar systems can all help inform the hazard identification process. Due to the complexity of modern systems, these methods will generally not be sufficient for HIA in isolation. We need more structured techniques to ensure we identify the full range of hazards and accident sequences. The choice of techniques depends on how much information is known about the system.

8. Where the system design is not (yet) known, we can use techniques such as Functional Failure Analysis (FFA or Functional FMEA) or Systems Theoretic Process Analysis (STPA). These can identify potential hazards based on descriptions of the system’s capability requirements, architecture or operating scenarios. These types of analyses can help set safety requirements and identify areas that will require more in-depth risk analysis as the design develops.

9. Bottom-up techniques such as Failure Mode Effects and Criticality Analysis (FMECA) and Hazard and Operability Studies (HAZOPS) can help us understand what system-level hazards might arise from component failures or process

deviations. Top-down techniques like Fault Tree Analysis (FTA) can identify combinations of events that could cause known hazards. Event Tree Analysis (ETA) can reveal the range of outcomes that could be caused by a given hazard. Use of these techniques requires a detailed understanding of the system's intended design and operation.

10. Once implementation details are known, more detailed analyses can be undertaken to identify common cause failures or human factors issues. When considering safety at a platform, system or compartment level, Zonal Hazard Analysis (ZHA) should be used to assess how various parts of a system might influence, or be influenced, by their surroundings. These surroundings could be either physical (equipment / human etc.) or environmental (temperature / humidity / wild life (bird strike, infestation) / pollution / sea etc.) Maintenance and procedural errors can be reviewed to establish any potential areas for concern, which could be missed if individual systems are only considered in isolation. The need to enter a hazardous area, for example to isolate the system electrically may be discovered using ZHA.

11. These analyses can be used in combination. They may also be carried out iteratively at different levels of the systems hierarchy. For instance, a FMECA might consider platform-level effects of generator failures (such as failing to provide an output, providing the incorrect voltage, or catching fire). If some of these failure modes are found to be critical, a FTA could be carried out on the generator design. This would investigate which combinations of component failures and other factors might cause the generator to fail.

12. Early in a project, risk analysis will be carried out at a high level, to influence the system requirements and design. As the design matures and subsystems and components are selected, it becomes feasible to carry out analysis in greater detail and at lower levels of the systems hierarchy. Again, the aim is to influence the design to reduce safety risk. When the system is in service, the risk analysis is reviewed to confirm that it is still valid, and further analysis may be needed to help plan modifications or investigate problems.

13. As projects progress and more information is known, it becomes possible to estimate risk with greater accuracy. While all the techniques mentioned above can be carried out qualitatively, some of them can also be carried out quantitatively or semi-quantitatively to give estimates of failure or occurrence rates. This may be necessary to support the risk estimation and risk control processes.

14. Whichever risk analysis techniques are used, the Safety and Environmental Management Plan (SEMP) should justify the choice of HAZID and HAZAN techniques. It should explain how they will be used to give the necessary level of information for risk assessment that supports decisions at different project stages. The results of the safety risk analysis itself must be recorded in the project's eCassandra hazard log.

Risk Assessment

15. Risk assessment is the bridge between identifying hazards and decisions about controlling the resultant risk. The first part is Risk Estimation (SMP06), using the outputs of risk analysis to derive an indication of the risk posed by different accident sequences. Risk and ALARP Evaluation (SMP07) is then used to decide if the risk must be reduced further, and whether the residual level of risk can be tolerated. Risk assessment can be qualitative, quantitative or, most likely, a combination of both

approaches. Qualitative approaches describe likelihood, severity and risk in general terms such as “improbable” or “high”. Even when clearly defined, these are open to a degree of interpretation. Semi-quantitative approaches use broad ranges of numbers. They are used when some mathematical analysis is required, but the values are not known with any degree of precision. Fully quantitative approaches are numeric and can support mathematic and statistical analysis. They are used when it is necessary to assess risk estimates against numeric targets, or to compare the cost-benefit of different risk control options.

16. In DE&S, qualitative or semi-quantitative risk assessment is often based on the use of a Risk Classification Matrix (RCM). Risks must be plotted on the project’s RCM according to their likelihood and severity, to give an estimate of the level of risk. This can then be used to prioritise action and more detailed assessment where necessary. A matrix is intended to give a broad indication of significance: the most important risks should be analysed in detail. Typically, this would include possible accidents with very severe consequences (e.g. multiple fatalities). A matrix will help to identify the most significant risks on which the Safety Case should concentrate. However, it should not normally be the only form of assessment for those risks. As the RCM does not provide an absolute measure of risk, action should be taken to validate and quantify risks that the RCM identifies as being in the upper regions. Note that a risk’s position on an RCM does not relate to whether it is ALARP. That depends on whether it is reasonably practicable to reduce the risk further.

17. The letter in each cell of the matrix defines a risk class (typically A, B, C or D), each of which has a level of authority for risk acceptance. Higher levels of risk must be communicated to the appropriate Duty Holder. Class A risks represent a very high level of risk, which can only be tolerated under truly exceptional circumstances. The definition of the matrix must be clearly recorded in the SEMP, including definitions of its likelihood and severity bands and their units of measurement.

18. For some low-risk systems, and for other systems early in the life cycle, risk assessment can be carried out in a qualitative or semi-quantitative manner; with targets set such as “no Class B or higher risks”. For many military systems, quantitative risk assessment will be required, supported by quantitative risk analysis techniques. This will be the case in the following circumstances:

- For complex systems, where engineering judgement is not sufficient to assess the significance of the hazards;
- When comparing different design solutions or risk reduction options, to support cost-benefit analysis; or
- For high risk systems, where more confidence is needed in the accuracy of risk estimates; and
- When comparing risk estimates against quantitative risk targets.

19. **Quantitative risk targets** address the likelihood of occurrence of specific identified accidents during a given time or number of operations, or the total risk to which individuals or groups may be exposed. They should be chosen to provide a measurable approach to the achievement of safety. Unrealistic or unmeasurable safety targets do not contribute to the safety process. They can lead to unnecessary project expense or an inability to verify that the requirements have been met.

20. Quantitative safety targets should be tailored for a specific system according to its function and nature. They should be recorded in the SEMP. Top-level safety targets may be based on the requirements in standards or regulation; historical knowledge of the achievable performance of similar systems; engineering judgement;

or a combination of all three. Targets for subsystems may also be set using the results of hazard analysis, based on their contribution to the safety of the higher-level system.

Risk Control

21. Guidance issued by the HSE describes how risks should be reduced to the lowest reasonably practicable level by taking preventative measures in order of priority. This hierarchy of control sets out the order to be followed when planning to reduce risks.

- Elimination – e.g. redesign the equipment or activity so that the hazard is removed or eliminated.
- Substitution – e.g. replace the material or process with a less hazardous one.
- Engineering controls – e.g. use work equipment or other measures to prevent falls where you cannot avoid working at height, install or use additional machinery to control risks from dust or fume, or separate the hazard from operators by methods such as enclosing or guarding dangerous items of machinery/equipment. Give priority to measures which protect collectively over individual measures.
- Administrative Controls (identifying and implementing procedures to achieve a safe working environment). e.g. reducing the time individuals are exposed to hazards (e.g. by job rotation); prohibiting use of mobile phones in hazardous areas; increasing safety signage.
- Personal protective clothes and equipment - Only after all the previous measures have been applied and found ineffective in controlling risks to an ALARP level must personal protective equipment (PPE) be used.

22. While administrative controls and PPE are important contributors to risk control, care must be taken to avoid becoming over-reliant on their effectiveness at achieving an ALARP state. When they are used, their effectiveness must be fully and realistically assessed with input from subject matter specialists and end users as necessary.

23. Control measures based on human intervention should be assessed in more detail to ensure that assumptions made about them are valid (e.g. the proposed mitigation is likely to be effective). This might involve an initial high-level Human Factors review that seeks to:

- Understand the precise performance criteria of the task (e.g. what is the person expected to do and under what conditions?);
- Identify and understand the cause of failure (e.g. error and error type or violation);
- Consider the suitability of the mitigation to address the specific error or violation that leads to the failure (e.g. training will not be an effective Risk Mitigation strategy against slip/lapse type errors); and
- Identify the key factors and how interventions will address them (e.g. if task complexity is an issue, consider ways to simplify the task through automation or other engineered options).

24. The output from the high-level review would support judgement on the viability of the risk mitigation option, for example:

- The Risk mitigation option is likely to be effective;

- The Risk mitigation option is unlikely to be effective in its current form, but might be suitable with additional or alternative Risk Mitigation measures;
- Any form of the Risk mitigation option is unlikely to lead to effective Risk Reduction. The risk should either be eliminated or engineered; or
- It is unclear whether the risk mitigation option will be effective. Further analysis may be needed, for example:
    - Mock up and test an emergency alarm and control system to check people can understand it and respond as intended;
    - Carry out a walkthrough of a task, to verify that it can be reliably completed within specified time limits;
    - Conduct Training Needs Analysis; and
    - Undertake workload analysis, to determine task manning and task design needs.

25. Further information on Human Factors assessment is available on the Knowledge in Defence Human Factors Integration pages. These include Technical Guide 7.3 on the Human Contribution to System Safety.

26. For the assessment to be valid, it must be based on the actual operating scenario. It requires input from individuals who have sufficient knowledge and awareness of the operating environment. This is particularly pertinent in-service (including normal use, maintenance and training) and in the disposal phase but should be considered throughout the lifecycle. Once systems have entered service, project teams must periodically seek feedback to ensure that they are still being operated in the way that has been assumed. If the operating environment or the way the system is used changes, the risk assessment will need to be updated.

27. The HSE recognises three approaches to making a claim that risk is ALARP:

- **Good practice arguments** demonstrate that risk control which measures comply with relevant good practice as defined in standards and guidance such as MOD Regulatory publications and ASEMS etc.
- **Qualitative arguments** based on common sense or professional judgement to weigh possible risk reduction against the necessary "sacrifice".
- **Quantitative arguments** based on numerical techniques such as Cost Benefit Analysis (CBA) to weigh possible risk reduction against the necessary "sacrifice".

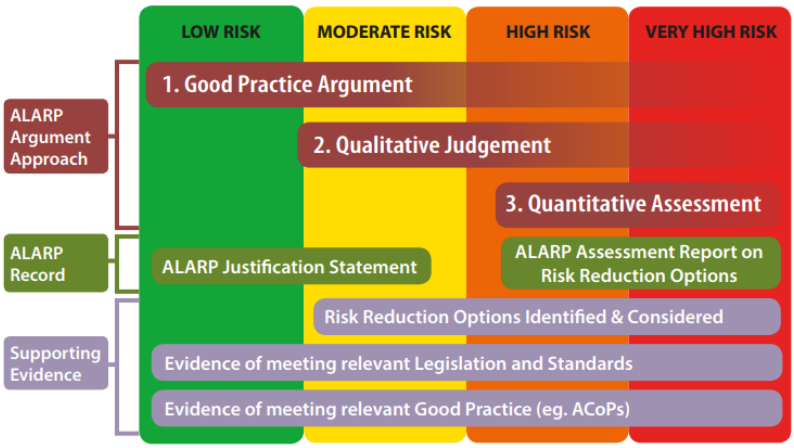

Figure 2. Approaches to ALARP Assessment

28. A good ALARP argument should provide a detailed justification of why the selected control measures represented the most practicable solution. It should also capture any additional or alternative control measures, and explain why they were not implemented. Reasons for discounting options might include grossly disproportionate expense or physical impracticability.

29. The validity of an ALARP argument can change at any stage in the lifecycle: assumptions can be discredited, technology can move on making previously-discounted mitigations viable. In addition, changes to configuration, usage, the operating environment and the operational envelope can introduce new hazards and accidents sequences. It is therefore essential that ALARP statements are robust and comprehensive in the first place but are also subjected to rigorous review which considers all aspects which may have an impact on their validity.

Personal Protective Equipment (PPE)

30. PPE is one means of preventing harm to the user. PPE selection should primarily be based on the hazards identified during the assessment. However, the selection of PPE must also reflect the working environment and not compromise the ability of the user to perform their duties. This includes considering the fit and comfort of the PPE. If either of these factors are not addressed, the likelihood of the user discarding the PPE is increased and arguments which assume its correct use are undermined.

31. PPE must be selected with the full involvement of the user community who must have full and current knowledge of the working environment. This extends to highlighting issues with prescribed PPE which may mean it is routinely discarded or worn in a manner outside its intended use.

Representation of the Safety Argument

32. The outputs from the risk management process will form a critical part of the safety argument for a system. As such, they must be recorded in the Safety Case Report (SCR) or Safety Assessment Report (SAR).

33. Several techniques can be used to provide a graphical representation of the safety argument, to help make it easier to understand and review. Two of the most commonly used are Goal Structured Notation (GSN) and Claims Argument Evidence (CAE). The advantage of both techniques is the ability to break complex safety arguments into manageable sections. They can help all interested parties understand how the safety argument has been constructed to meet the top-level claim.

34. Bow Tie diagrams can also be useful to visualise accident sequences and the barriers and controls that are in place to prevent hazardous events occurring or progressing to accidents.

35. Various software tools exist to support these graphical techniques, ranging from simple drawing packages to sophisticated products that can organise Safety Case documentation, link to Hazard Analysis tools and automatically generate documents and summary reports.

36. During a project lifecycle, several iterations of the SCR or SAR will be required for the system to pass major project milestones such as Initial Gate, Main Gate, System Acceptance and introduction of a mid-life update. These milestones will

provide the measurement points at which the achievement of safety requirements by the system can be reviewed and confirmed. Periodic updates will also be required during the In-service phase to ensure the SCR remains valid considering all changes to configuration, usage environment and any aging effects. Honest user feedback is vital to ensure the in-service safety case continues to reflect the actual state of the equipment and how it is used.